March 2013

MONTHLY
Cyber Security
Newsletter

Security Tips

Training Opportunities Coming Soon:

Web Application Security March 18, 2013

ITIL Awareness April 15, 2013

http://www.its.ms.g ov/Services/Pages /Security-Training-Opportunities.aspx

		ON A
	100 mg 10	C
- 177 T	2003 100 100 100 100 100 100 100 100 100	
12 (12 (12 (12 (12 (12 (12 (12 (12 (12 (1
1312 70 1000 01		00-0
3653-30 1500-19 974-03	1620 63 20	
#34.60 379.60 100 #4142-51 11916-70 21355		
16230-81	\$622AA.81 8120.00 2A036.00	UM
300-50 80475		MIC
		* *
1000 mg	24036 00 8609.91 16640 26	
1733-02 117-54	240	CF
1363-747 12-18 2804	73 91	
226-14 64- 110-74 134	742305-73 16540-560 8609-97 16540-29 8609-97	a 1988
407-25 217-53 243-34 230-50 419-09 523-4		
813-60 293-59 533-60	7580	
06-56 1615-28 2936-95 5500-61	001 931 661	58494
06-58 1615-28 2936-95 5500-61 8-25 533-90 970-72 1213-39	2000 30 122 80	THE SECOND
8587-52	202400-300 1227-300 393464-37-39 94979-80	22
90 9875-64 17297-93 23759-61	35007-350	22
6 325835-34 583266-30 800065-59	759071769	
	4891	38
		13 105
	2514311 184808	3.28 63
700-	2514431 184800 62 4818	3328 100 380500 143811 66611411 143811
39-89 21720-15	7080-24	805-00-143
	41	0714
20-15 1167-47	2301-48	666,
67-47 3955-27	2690-30	
	2923-00	STORE-
	2923-00	Mary Tree
5338-00		The second second
8-00	-506.82	TO SERVICE STATE OF THE PARTY O
	28596-82	100
29369-49	5606-76	THE REAL PROPERTY.
29300	000	
9-49 9707-15		
7-15		
	106395-34	

Mississippi Department of Information Technology Services

Division of Information Security

Protect Yourself from Email Tax Scams

It's tax season and criminals are seizing the opportunity for scams. Don't become the next victim.

Scammers leverage every means at their disposal to separate you from your money, your identity, or anything else of value they can get. They may offer seemingly legitimate "tax services" designed to steal your identity and your tax refund, sometimes with the lure of bigger write-offs or refunds. Scams may include mocked up websites and tax forms that look like they belong to the IRS to trick you into providing your personal information.

Scam artists can prey on users by promising refunds that are fraudulent, a scam the IRS says has been rampant in previous years. In these scams, notices are posted on bulletin boards, in libraries, and at other community sites where people visit either in person or online. Scammers make money from this trick in two ways: first, they collect a fee for helping to "file" for a refund on behalf of their victims, and then they steal the victim's identity for further exploitation. The victims are left paying a fee for a fraudulent service, not getting a refund they thought they would, and are potentially in a position to face charges for failing to file a return or for committing fraudulent reporting.

How to Recognize an Email Tax Scam

According to the IRS, below are the key ways to recognize an email tax scam. The email:

- requests personal and/or financial information, such as name, SSN, bank or credit card
 account numbers or security-related information, such as mother's maiden name, either
 in the email itself or on another site to which a link in the email directs you;
- includes exciting offers to get you to respond, such as mentioning a tax refund or offering to pay you to participate in an IRS survey;
- threatens a consequence for not responding to the email, such as additional taxes or blocking access to your funds;
- has incorrect spelling for the Internal Revenue Service or other federal agencies;
- uses incorrect grammar or odd phrasing;
- discusses "changes to tax laws" that include a downloadable document (usually in PDF format) that purports to explain the new tax laws (these downloads are populated with malware that, once downloaded, may infect your computer).

this newsletter is brought to you by...



www.msisac.org



www.its.ms.gov

How To Avoid Becoming A Victim

To stay safer this tax season, follow these five steps:

- Secure your computer. If your computer does not have proper security controls, it is
 vulnerable to access by criminals, who may be able to steal information stored on it.
 Make sure your computer has the latest security updates installed. Check that your
 anti-virus and anti-spyware software are running properly and are receiving automatic
 updates from the vendor. If you haven't already done so, install and enable a firewall.
- 2. Carefully select the sites you visit. Safely searching for tax forms, advice on deductibles, tax preparers, and other similar topics requires caution. Know the site. Know the company. Do not visit a site by clicking on a link sent in an email, found on someone's blog, or on an advertisement. The website you land on may look just like the real site, but it may be a well-crafted fake.
- 3. Don't fall prey to email, web, or social networking scams. Common scams tout tax rebates, offer great deals on tax preparation or offer a free tax calculator tool. If you did not solicit the information, it's likely a scam. If the email claims to be from the IRS, it's a scam the IRS will not contact you via email, text messaging or your social network, nor does it advertise on websites. If the email appears to be from your employer, bank, broker, etc. claiming there is an issue with what they reported for you and you need to verify some information, it might be a scam. Do not respond to the email. Contact the entity directly before responding.
- 4. **Never send sensitive information in an email.** It may be intercepted and read by criminals.
- 5. Use strong passwords. Cyber criminals have developed programs that automate the ability to guess your passwords. To protect yourself, passwords must be difficult for others to guess, but at the same time, easy for you to remember. Passwords should have a minimum of nine characters and include upper case (capital letters), lowercase letters, numbers, and symbols. Make sure your work passwords are different from your personal passwords.

For More Information:

For additional information about tax related scams and identity theft, please visit:

- Taxpayer Guide to Identity Theft: www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft
 Theft
- Tax Scams/Consumer Alerts: www.irs.gov/uac/Tax-Scams-Consumer-Alerts
- IRS Releases the Dirty Dozen Tax Scams for 2012: www.irs.gov/uac/IRS-Releases-the-Dirty-Dozen-Tax-Scams-for-2012
- What's Hot IRS: www.irs.gov/uac/What's-Hot
- Report Phishing: www.irs.gov/uac/Report-Phishing

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.